



Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Journal of Number Theory 98 (2003) 432–437

JOURNAL OF
**Number
Theory**

<http://www.elsevier.com/locate/jnt>

Existence of certain fundamental discriminants and class numbers of real quadratic fields[☆]

Dongho Byeon

School of Mathematical Sciences, Seoul National University, Seoul, South Korea

Received 18 April 2002; revised 17 June 2002

1. Introduction and statement of results

Let D be the fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, $h(D)$ its class number, and $\chi_D := (\frac{D}{\cdot})$ the usual Kronecker character. Let p be prime, \mathbb{Z}_p the ring of p -adic integers, and $\lambda_p(\mathbb{Q}(\sqrt{D}))$ the Iwasawa λ -invariant of the cyclotomic \mathbb{Z}_p -extension of $\mathbb{Q}(\sqrt{D})$. Let $R_p(D)$ denote the p -adic regulator of $\mathbb{Q}(\sqrt{D})$, and $|\cdot|_p$ denote the usual multiplicative p -adic valuation normalized so that $|p|_p = \frac{1}{p}$.

In [9], by applying Sturm's theorem on the congruence of modular forms to Cohen's half-integral weight modular forms, Ono proved the following theorem.

Theorem (Ono [9]). *Let $p > 3$ be prime. If there is a fundamental discriminant D_0 coprime to p for which*

- (i) $(-1)^{\frac{p-1}{2}} D_0 > 0$,
- (ii) $|B(\frac{p-1}{2}, \chi_{D_0})|_p = 1$,

where $B(\frac{p-1}{2}, \chi_{D_0})$ is the $\frac{p-1}{2}$ -st generalized Bernoulli number with character χ_{D_0} , then

$$\#\left\{0 < D < X \mid h(D) \not\equiv 0 \pmod{p}, \chi_D(p) = 0, \text{ and } \left| \frac{R_p(D)}{\sqrt{D}} \right|_p = 1\right\} \gg_p \frac{\sqrt{X}}{\log X}.$$

Ono also checked that conditions (i) and (ii) hold for all primes $3 < p < 5000$ using MAPLE.

[☆]This work was supported by Korea Research Foundation Grant KRF-2002-003-C00001.

E-mail address: dhbyeon@math.snu.ac.kr.

In this note, we shall prove that conditions (i) and (ii) in the above theorem hold for any prime $p > 3$ and obtain the following theorem.

Theorem 1.1. *Let $p > 3$ be prime.*

(a) *If $p \equiv 1 \pmod{4}$, then the fundamental discriminant $D_0 > 0$ of the real quadratic field $\mathbb{Q}(\sqrt{p-2})$ satisfies conditions (i) and (ii).*

(b) *If $p \equiv 3 \pmod{4}$, then the fundamental discriminant $D_0 < 0$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{-(p-4)})$ satisfies conditions (i) and (ii).*

From the above Ono's theorem and Theorem 1.1, we immediately have the following corollary.

Corollary 1.2. *Let $p > 3$ be prime. Then*

$$\#\left\{0 < D < X \mid h(D) \not\equiv 0 \pmod{p}, \chi_D(p) = 0, \text{ and } \left| \frac{R_p(D)}{\sqrt{D}} \right|_p = 1\right\} \gg_p \frac{\sqrt{X}}{\log X}.$$

From a theorem of Iwasawa [7] and Corollary 1.2, we also immediately have the following corollary.

Corollary 1.3. *Let $p > 3$ be prime. Then*

$$\#\{0 < D < X \mid \lambda_p(\mathbb{Q}(\sqrt{D})) = 0, \chi_D(p) = 0\} \gg_p \frac{\sqrt{X}}{\log X}.$$

Remark 1. In [2], by refining Ono's method and using similar method to this note, the author proved the following theorem and corollary.

Theorem. *Let $p > 3$ be prime and $\delta = -1$ or 1 . If $\delta = -1$, then for any $p \equiv 3 \pmod{4}$, and if $\delta = 1$, then for any p ,*

$$\#\left\{0 < D < X \mid h(D) \not\equiv 0 \pmod{p}, \chi_D(p) = \delta, \text{ and } |R_p(D)|_p = \frac{1}{p}\right\} \gg_p \frac{\sqrt{X}}{\log X}.$$

Corollary. *Let $p > 3$ be prime and $\delta = -1$ or 1 . If $\delta = -1$, then for any $p \equiv 3 \pmod{4}$, and if $\delta = 1$, then for any p ,*

$$\#\{0 < D < X \mid \lambda_p(\mathbb{Q}(\sqrt{D})) = 0, \chi_D(p) = \delta\} \gg_p \frac{\sqrt{X}}{\log X}.$$

However, the case of $\delta = -1$ and $p \equiv 1 \pmod{4}$ is a remaining problem.

Remark 2. Similar works for imaginary quadratic fields can be found in [1,3–5,8,10].

2. Proof of Theorem 1.1

Let $p > 3$ be prime and $D_p := (-1)^{\frac{p-1}{2}} pD$. In the proof of Proposition 2 in [9], by using the construction of Kubota–Leopoldt p -adic L -function, the Kummer congruences, and the p -adic class number formula, Ono proved that

$$-\frac{2B(\frac{p-1}{2}, \chi_D)}{p-1} \equiv \frac{2h(D_p)R_p(D_p)}{\sqrt{D_p}} \pmod{p}.$$

Note that D_0 clearly satisfies condition (i) in the above Ono's Theorem. Therefore, to prove Theorem 1.1, it is enough to show that $\left| \frac{h(D_{0p})R_p(D_{0p})}{\sqrt{D_{0p}}} \right|_p = 1$, that is,

$$(1) \quad h(D_{0p}) \not\equiv 0 \pmod{p},$$

$$(2) \quad \left| \frac{R_p(D_{0p})}{\sqrt{D_{0p}}} \right|_p = 1.$$

Proof of (1). Let $D > 0$ be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$ and $L(s, \chi_D)$ be the Dirichlet L -function with character χ_D . Hua [6, Theorem 13.3, p. 328] obtained the following upper bound for $L(1, \chi_D)$:

$$L(1, \chi_D) < \frac{\log D}{2} + 1.$$

Dirichlet's class number formula says that

$$h(D) = \frac{\sqrt{D}L(1, \chi_D)}{2 \log \varepsilon_D},$$

where $\varepsilon_D > 1$ is the fundamental unit of $\mathbb{Q}(\sqrt{D})$.

Thus, by the above Hua's upper bound for $L(1, \chi_D)$, we have that

$$h(D) < \sqrt{D} \cdot \frac{(2 + \log \sqrt{D})}{4 \log \varepsilon_D} < \sqrt{D} \cdot \frac{(2 + \log \sqrt{D})}{2 \log(D/4)},$$

because $\varepsilon_D > \sqrt{D}/2$.

Since D_{0p} is the fundamental discriminant of the real quadratic fields $\mathbb{Q}(\sqrt{p(p-2)})$ or $\mathbb{Q}(\sqrt{p(p-4)})$, we have

$$h(D_{0p}) < p$$

and we proved that $h(D_{0p}) \not\equiv 0 \pmod{p}$. \square

Proof of (2). Let $D > 0$ be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$ and $\varepsilon_D > 1$ its fundamental unit. Then $R_p(D) = \log_p(\varepsilon_D)$. Let $p > 3$ be prime and \mathfrak{p} a prime ideal of $\mathbb{Q}(\sqrt{D})$ over p . Let $n(p, D)$ be a nonnegative integer satisfying that

$$\mathfrak{p}^{n(p,D)} \mid (\varepsilon_D^{N(\mathfrak{p})-1} - 1) \text{ but } \mathfrak{p}^{n(p,D)+1} \nmid (\varepsilon_D^{N(\mathfrak{p})-1} - 1),$$

where N is the absolute norm of $\mathbb{Q}(\sqrt{D})$. Note that $n(p, D) \geq 1$. Since $|\varepsilon_D^{N(\mathfrak{p})-1} - 1|_p = |\log_p(\varepsilon_D^{N(\mathfrak{p})-1})|_p$, we have that

$$|R_p(D)|_p = \begin{cases} p^{-n(p,D)} & \text{if } p \text{ is unramified,} \\ p^{-n(p,D)/2} & \text{if } p \text{ is ramified.} \end{cases}$$

Since D_{0p} is the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{p(p-2)})$ or $\mathbb{Q}(\sqrt{p(p-4)})$, we have $|\sqrt{D_{0p}}|_p = p^{-\frac{1}{2}}$. Thus, from the above argument, to prove (2), it is enough to show that

$$n(p, D_{0p}) = 1.$$

First we consider the case $p \equiv 1 \pmod{4}$ and D_{0p} is the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{p(p-2)})$. Let $\varepsilon_{D_{0p}} > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{p(p-2)})$ and $\alpha := (p-1) + \sqrt{p(p-2)}$. Since $N_{\mathbb{Q}(\sqrt{D_{0p}})/\mathbb{Q}}(\alpha) = 1$ and $\alpha > 1$, $\alpha = \varepsilon_{D_{0p}}^j$ for some positive integer j .

Let \mathfrak{p} be a prime ideal of $\mathbb{Q}(\sqrt{D_{0p}})$ over p , i.e., $p = \mathfrak{p}^2$. Then, by easy computation, we have

$$\varepsilon_{D_{0p}}^{2j} - 1 = \alpha^2 - 1 = ((p-1) + \sqrt{p(p-2)})^2 - 1 \equiv 0 \pmod{\mathfrak{p}},$$

$$\varepsilon_{D_{0p}}^{2j} - 1 = \alpha^2 - 1 = ((p-1) + \sqrt{p(p-2)})^2 - 1 \not\equiv 0 \pmod{\mathfrak{p}^2 = p}.$$

Now we claim that

$$\varepsilon_{D_{0p}}^{N(p)-1} - 1 = \varepsilon_{D_{0p}}^{p-1} - 1 \not\equiv 0 \pmod{\mathfrak{p}^2}.$$

Suppose that $\varepsilon_{D_{0p}}^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}^2}$. Since $\varepsilon_{D_{0p}}^{2j} - 1 \equiv 0 \pmod{\mathfrak{p}}$, we have $2j|(p-1)$ or $(p-1)|2j$. If $(p-1)|2j$, then clearly $\varepsilon_{D_{0p}}^{2j} - 1 \equiv 0 \pmod{\mathfrak{p}^2}$ and we have a contradiction. If $2j|(p-1)$, write $p-1 = m \cdot 2j$ and

$$\varepsilon_{D_{0p}}^{p-1} - 1 = (\varepsilon_{D_{0p}}^{2j} - 1)((\varepsilon_{D_{0p}}^{2j})^{m-1} + \cdots + 1).$$

Since $\varepsilon_{D_{0p}}^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}^2}$ and $(\varepsilon_{D_{0p}}^{2j})^{m-1} + \cdots + 1 \equiv m \not\equiv 0 \pmod{\mathfrak{p}}$, we also have $\varepsilon_{D_{0p}}^{2j} - 1 \equiv 0 \pmod{\mathfrak{p}^2}$ and a contradiction. Thus we showed the claim and proved $n(p, D_{0p}) = 1$.

Finally we consider the case $p \equiv 3 \pmod{4}$ and D_{0p} is the fundamental discriminant of $\mathbb{Q}(\sqrt{p(p-4)})$. In this case, if we let $\alpha := \frac{p-2}{2} + \frac{\sqrt{p(p-4)}}{2}$, then by the same method, we can also prove $n(p, D_{0p}) = 1$. \square

Remark 3. A careful analysis of the proof of Theorem 2 in [9] produces a much more explicit result than Corollary 1.2 as follows:

If $p > 3$ is a prime and $\varepsilon > 0$, for all sufficiently large $X > 0$,

$$\# \left\{ 0 < D < X \mid h(D) \not\equiv 0 \pmod{p}, \chi_D(p) = 0, \text{ and } \left| \frac{R_p(D)}{\sqrt{D}} \right|_p = 1 \right\} \\ \geq (c(p) - \varepsilon) \frac{\sqrt{X}}{\log X}$$

with $c(p) = 1/(2^{(\pi(\kappa(p))-1)} \cdot \sqrt{\kappa(p)p})$, where $\pi(x)$ is the number of primes not exceeding x and $\kappa(p) := p^2 Q^3(p+1)(Q+1)/4$ in the proof of Theorem 2 in [9].

From this and from our exact choice of D_0 in Theorem 1.1, we can obtain

$$c(p) \geq 1/(2^{(\pi(p^7/4)-2)} \cdot p^4),$$

since $Q < p - 2$ if $p \equiv 1 \pmod{4}$ and $Q < p - 4$ if $p \equiv 3 \pmod{4}$ except $p = 5$ or 7 . When $p = 5$, let $Q = 7$ and when $p = 7$, let $Q = 5$. Then we have $c(5) \geq 1/(2^{9846} \cdot 35 \cdot \sqrt{105})$ and $c(7) \geq 1/(2^{7257} \cdot 35 \cdot \sqrt{105})$.

Acknowledgments

The author thanks Professor Hendrik Lenstra for finding a mistake in this manuscript. The author also thanks the referee for many helpful suggestions.

References

- [1] D. Byeon, A note on the basic Iwasawa λ -invariants of imaginary quadratic fields and congruence of modular forms, *Acta Arith.* 89 (1999) 295–299.
- [2] D. Byeon, Indivisibility of class numbers and Iwasawa λ -invariants of real quadratic fields, *Compositio Math.* 126 (2001) 249–256.
- [3] P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, *J. Number Theory* 6 (1974) 276–278.
- [4] K. Horie, A note on basic Iwasawa λ -invariants of imaginary quadratic fields, *Invent. Math.* 88 (1987) 31–38.

- [5] K. Horie, Y. Onishi, The existence of certain infinite families of imaginary quadratic fields, *J. Reine Angew. Math.* 390 (1988) 97–113.
- [6] L.-K. Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin–New York, 1982.
- [7] K. Iwasawa, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* 20 (1956) 257–258.
- [8] W. Kohnen, K. Ono, Indivisibility of class numbers of imaginary quadratic fields and orders of Tate–Shafarevich groups of elliptic curves with complex multiplication, *Invent. Math.* 135 (1999) 387–398.
- [9] K. Ono, Indivisibility of class numbers of real quadratic fields, *Compositio Math.* 119 (1999) 1–11.
- [10] K. Ono, C. Skinner, Fourier coefficients of half-integral weight modular forms modulo l , *Ann. Math.* 147 (1998) 453–470.